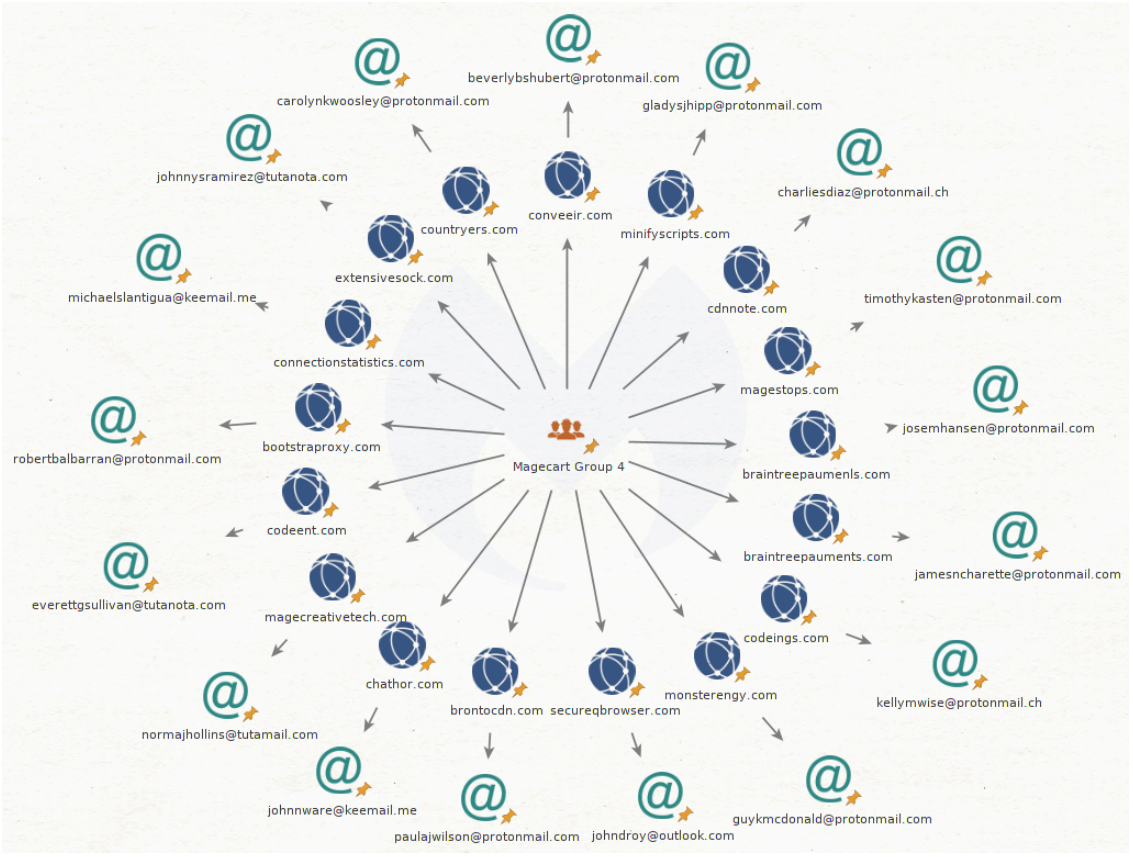
Magecart Group 4: A link with Cobalt Group?

By Threat Intelligence Team

Published: 2019-10-02 · Archived: 2026-04-05 22:57:10 UTC



About Cobalt Group

Cobalt Group came to the forefront of public attention in summer 2016 with their “jackpotting” attacks against financial institutions in Europe, which reportedly netted the group over $3 million. Since that time, they have purportedly amassed over a billion dollars from global institutions, evolving their tactics, techniques, and procedures as they go.

Cobalt Domain Registration and other TTPs

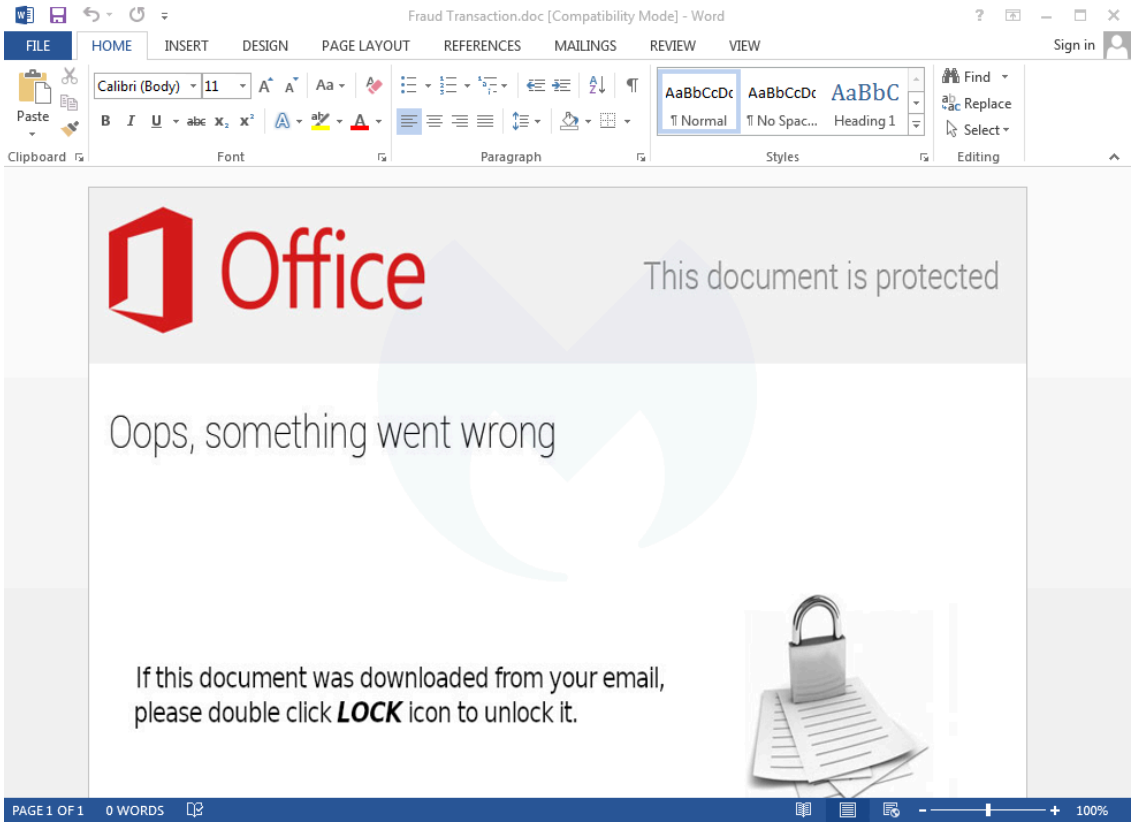
While changing tactics as they have evolved, an identifiable pattern in email naming conventions historically used by Cobalt allowed HYAS to not only identify previous campaign domains, but helped link Cobalt Group campaigns to the Magecart domains identified above.

A small shift from one of their previous conventions of [firstname],[lastname], [fournumbers] (overwhelmingly using protonmail accounts, with a handful of tutanota/keemail.me email accounts) changed to the above-noted

convention of [firstname], [initial], [lastname] again using the same email services and registrars, and notably the same use of privacy protection services.

Given the use of privacy services for all the domains in question, it is highly unlikely that this naming convention would be known to any other actor besides those who registered both the Cobalt Group and Magecart infrastructure. In addition, further investigation revealed that regardless of the email provider used, 10 of the seemingly separate accounts reused only two different IP addresses, even over weeks and months between registrations.

One of those emails is petersmelanie@protonmail.com, which was used to register 23 domains, including my1xbet[.]top. This domain was used in a phishing campaign leveraging CVE-2017-0199 with a decoy document called Fraud Transaction.doc.



The same petersmelanie@protonmail.com also registered oracle-business[.]com. Similar campaigns against Oracle and various banks have been attributed to Cobalt Group, with, for example, the domain oracle-system[.]com.

A growing threat requires ongoing work

Based on their historical ties to the space, and the entrance of sophisticated actor groups such as FIN6 and others, it's logical to conclude that Cobalt Group would also enter this field and continue to diversify their criminal efforts against global financial institutions.

The use of both client-side and server-side skimmers and the challenges this poses in identifying Magecart compromises by advanced threat groups necessitates the ongoing work of industry partners to help defend against

this significant and growing threat. On that note, the authors of this post would like to recognize the substantial contribution that industry researchers and law enforcement officials are making to combat groups like Cobalt, and hope that the information contained within adds to this corpus of knowledge and further strengthens these efforts.

Indicators of Compromise (IOCs)

Client-side skimmer

urlscan.io archive

Server-side skimmer

urlscan.io archive

Registrant emails associated with Magecart Group 4 domains

robertbalbarran@protonmail.com
josemhansen@protonmail.com
jamesncharette@protonmail.com
paulajwilson@protonmail.com
charliesdiaz@protonmail.ch
johnnware@keemail.me
everettgsullivan@tutanota.com
kellymwise@protonmail.ch
michaelslantigua@keemail.me
beverlybshubert@protonmail.com
carolynkwoosley@protonmail.com
johnnysramirez@tutanota.com
normajhollins@tutamail.com
timothykasten@protonmail.com
gladysjhipp@protonmail.com
guykmcdonald@protonmail.com
johndroy@outlook.com

Registrant emails associated with Cobalt domains

petersmelanie@protonmail.com
jasoncantrell1996@protonmail.com

Cobalt domains registered with Magecart email naming convention

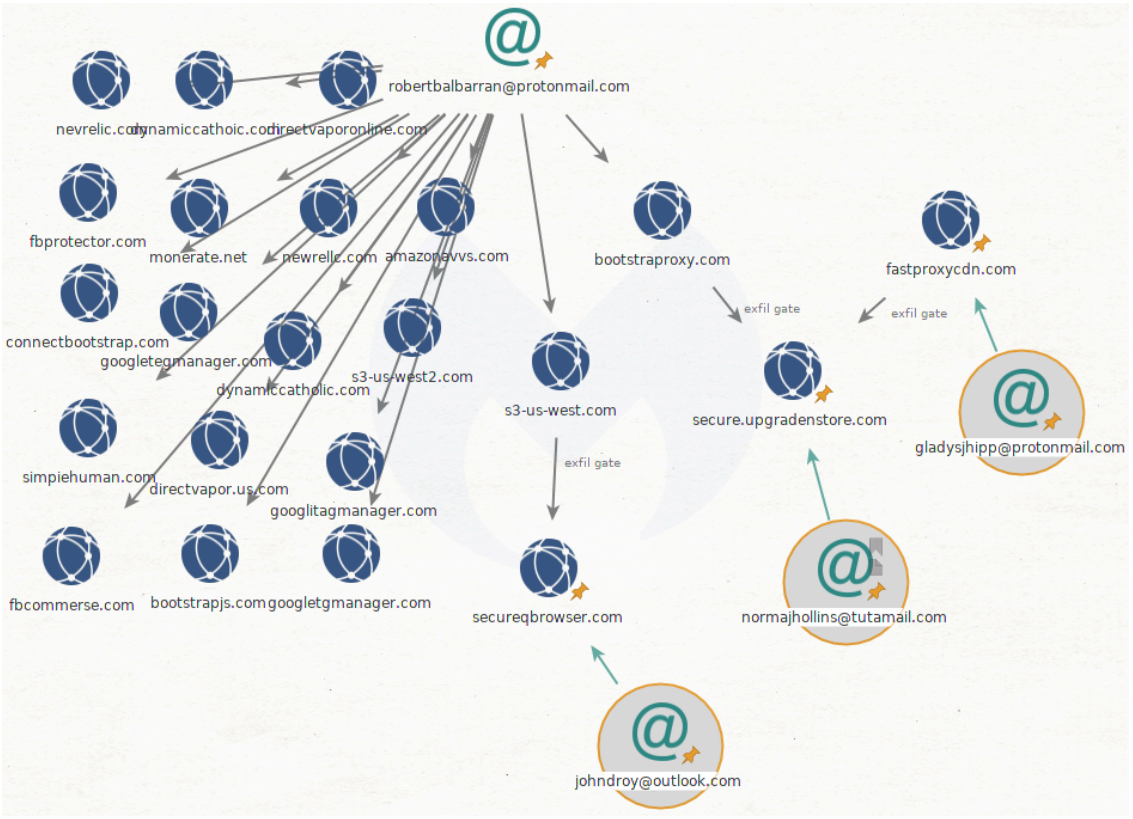
oracle-business[.]com
my-1xbet[.]com
sbeibank[.]online
curacaoegaming[.]site
my1xbet[.]top

newreg[.]site
sbepbank[.]com
orkreestr[.]com
orkreestr[.]host
sbersafe[.]top
aoreestr[.]site
newreg[.]host
sbeibank[.]com
sbelbank[.]com
aoreestr[.]online
curacaoegaming[.]online
sbepbank[.]online
sbelbank[.]online
curacao-egaming[.]online
my1xbet[.]online
orkreestr[.]press
newreg[.]online
aoreestr[.]com

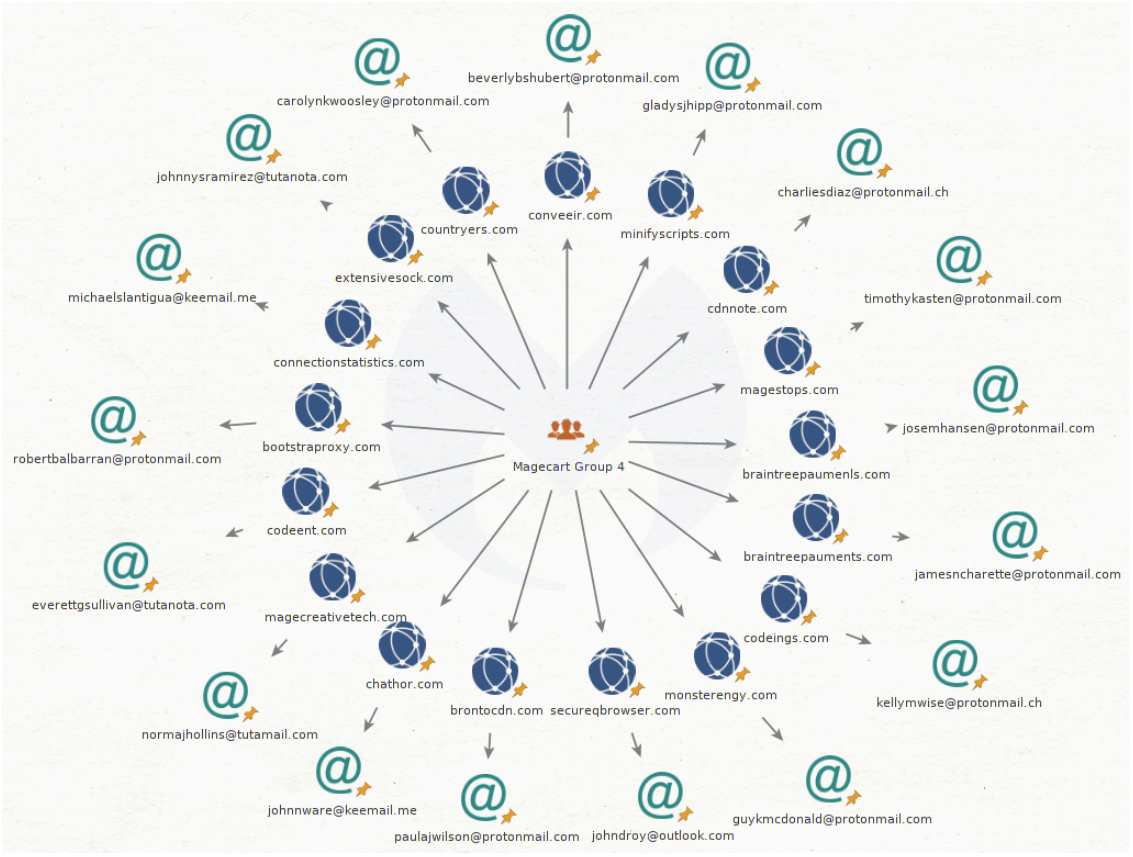
Previous FIN7 domains identified through naming conventions

akamaiservice-cdn[.]com
appleservice-cdn[.]com
bing-cdn[.]com
booking-cdn[.]com
cdn-googleapi[.]com
cdn-skype[.]com
cdn-yahooapi[.]com
cdnj-cloudflare[.]com
cisco-cdn[.]com
cloudflare-cdn-r5[.]com
digicert-cdn[.]com
exchange-cdn[.]com
facebook77-cdn[.]com
globaltech-cdn[.]com
gmail-cdn3[.]com
googl-analytic[.]com
google-services-s5[.]com
hpservice-cdn[.]com
infosys-cdn[.]com
instagram-cdn[.]com
live-cdn2[.]com
logitech-cdn[.]com

msdn-cdn[.]com
msdn-update[.]com
mse-cdn[.]com
mse-cdn[.]com
pci-cdn[.]com
realtek-cdn[.]com
servicebing-cdn[.]com
servicebing-cdn[.]com
testing-cdn[.]com
tw32-cdn[.]com
vmware-cdn[.]com
windowsupdatemicrosoft[.]com
yahooservices-cdn[.]com



Email addresses used to register Magecart domains belonging to Magecart Group 4 contain a [first name], [initial], and [last name]. Expanding our search to other domains used by Group 4 and searching through HYAS' Comox data set, we see this trend continues:



About Cobalt Group

Cobalt Group came to the forefront of public attention in summer 2016 with their “jackpotting” attacks against financial institutions in Europe, which reportedly netted the group over $3 million. Since that time, they have purportedly amassed over a billion dollars from global institutions, evolving their tactics, techniques, and procedures as they go.

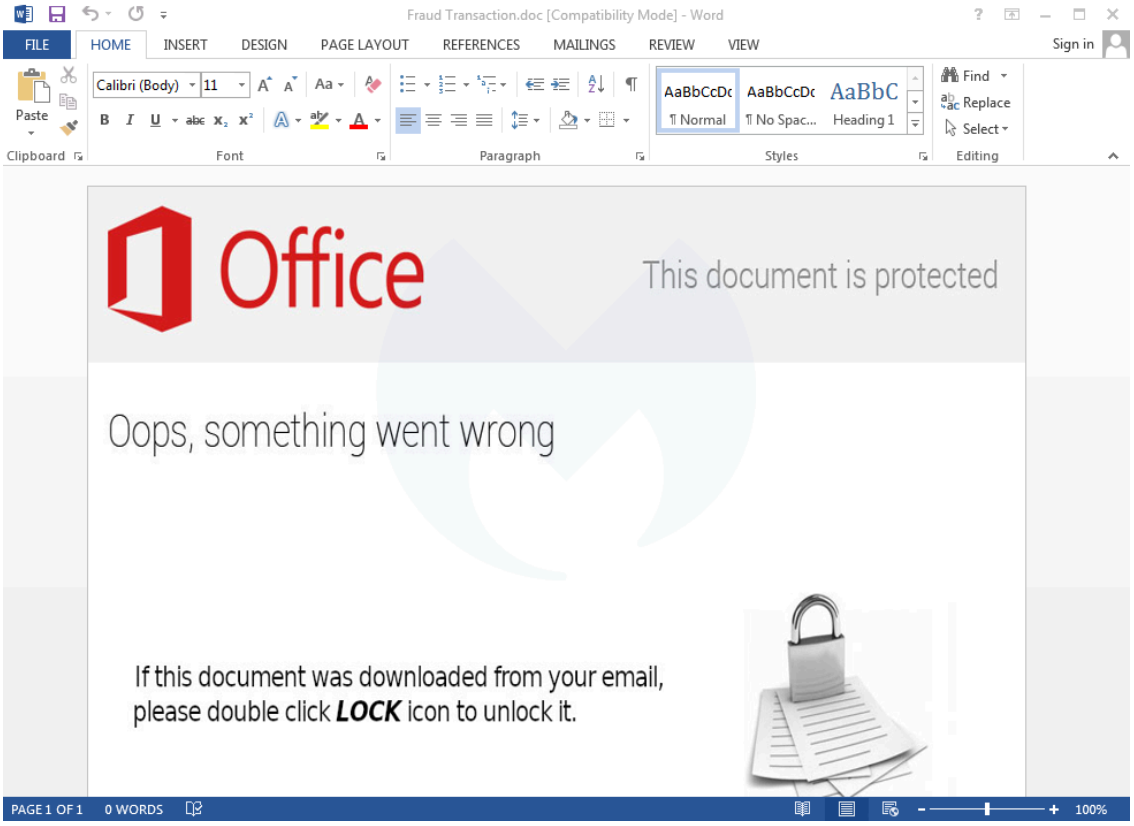
Cobalt Domain Registration and other TTPs

While changing tactics as they have evolved, an identifiable pattern in email naming conventions historically used by Cobalt allowed HYAS to not only identify previous campaign domains, but helped link Cobalt Group campaigns to the Magecart domains identified above.

A small shift from one of their previous conventions of [firstname],[lastname], [fournumbers] (overwhelmingly using protonmail accounts, with a handful of tutanota/keemail.me email accounts) changed to the above-noted convention of [firstname], [initial], [lastname] again using the same email services and registrars, and notably the same use of privacy protection services.

Given the use of privacy services for all the domains in question, it is highly unlikely that this naming convention would be known to any other actor besides those who registered both the Cobalt Group and Magecart infrastructure. In addition, further investigation revealed that regardless of the email provider used, 10 of the seemingly separate accounts reused only two different IP addresses, even over weeks and months between registrations.

One of those emails is petersmelanie@protonmail.com, which was used to register 23 domains, including my1xbet[.]top. This domain was used in a phishing campaign leveraging CVE-2017-0199 with a decoy document called Fraud Transaction.doc.



The same petersmelanie@protonmail.com also registered oracle-business[.]com. Similar campaigns against Oracle and various banks have been attributed to Cobalt Group, with, for example, the domain oracle-system[.]com.

A growing threat requires ongoing work

Based on their historical ties to the space, and the entrance of sophisticated actor groups such as FIN6 and others, it's logical to conclude that Cobalt Group would also enter this field and continue to diversify their criminal efforts against global financial institutions.

The use of both client-side and server-side skimmers and the challenges this poses in identifying Magecart compromises by advanced threat groups necessitates the ongoing work of industry partners to help defend against this significant and growing threat. On that note, the authors of this post would like to recognize the substantial contribution that industry researchers and law enforcement officials are making to combat groups like Cobalt, and hope that the information contained within adds to this corpus of knowledge and further strengthens these efforts.

Indicators of Compromise (IOCs)

Client-side skimmer

urlscan.io archive

Server-side skimmer

urlscan.io archive

Registrant emails associated with Magecart Group 4 domains

robertbalbarran@protonmail.com
josemhansen@protonmail.com
jamesncharette@protonmail.com
paulajwilson@protonmail.com
charliesdiaz@protonmail.ch
johnnware@keemail.me
everettgsullivan@tutanota.com
kellymwise@protonmail.ch
michaelslantigua@keemail.me
beverlybshubert@protonmail.com
carolynkwoosley@protonmail.com
johnnysramirez@tutanota.com
normajhollins@tutamail.com
timothykasten@protonmail.com
gladysjhipp@protonmail.com
guykmcdonald@protonmail.com
johndroy@outlook.com

Registrant emails associated with Cobalt domains

petersmelanie@protonmail.com
jasoncantrell1996@protonmail.com

Cobalt domains registered with Magecart email naming convention

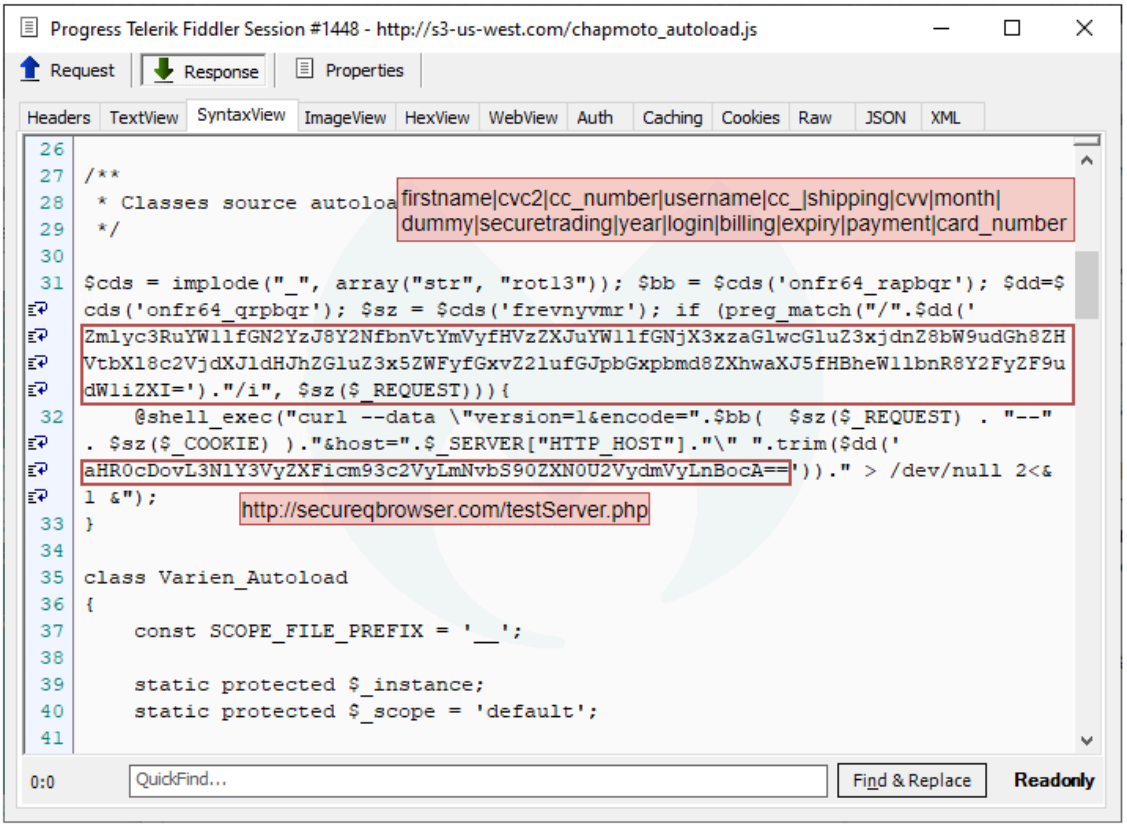
oracle-business[.]com
my-1xbet[.]com
sbeibank[.]online
curacaoegaming[.]site
my1xbet[.]top
newreg[.]site
sbepbank[.]com
orkreestr[.]com
orkreestr[.]host
sbersafe[.]top
aoreestr[.]site
newreg[.]host
sbeibank[.]com
sbelbank[.]com

aoreestr[.]online
curacaoegaming[.]online
sbepbank[.]online
sbelbank[.]online
curacao-egaming[.]online
my1xbet[.]online
orkreestr[.]press
newreg[.]online
aoreestr[.]com

Previous FIN7 domains identified through naming conventions

akamaiservice-cdn[.]com
appleservice-cdn[.]com
bing-cdn[.]com
booking-cdn[.]com
cdn-googleapi[.]com
cdn-skype[.]com
cdn-yahooapi[.]com
cdnj-cloudflare[.]com
cisco-cdn[.]com
cloudflare-cdn-r5[.]com
digicert-cdn[.]com
exchange-cdn[.]com
facebook77-cdn[.]com
globaltech-cdn[.]com
gmail-cdn3[.]com
googl-analytic[.]com
google-services-s5[.]com
hpservice-cdn[.]com
infosys-cdn[.]com
instagram-cdn[.]com
live-cdn2[.]com
logitech-cdn[.]com
msdn-cdn[.]com
msdn-update[.]com
mse-cdn[.]com
mse-cdn[.]com
pci-cdn[.]com
realtek-cdn[.]com
servicebing-cdn[.]com
servicebing-cdn[.]com
testing-cdn[.]com

tw32-cdn[.]com
vmware-cdn[.]com
windowsupdatemicrosoft[.]com
yahooservices-cdn[.]com

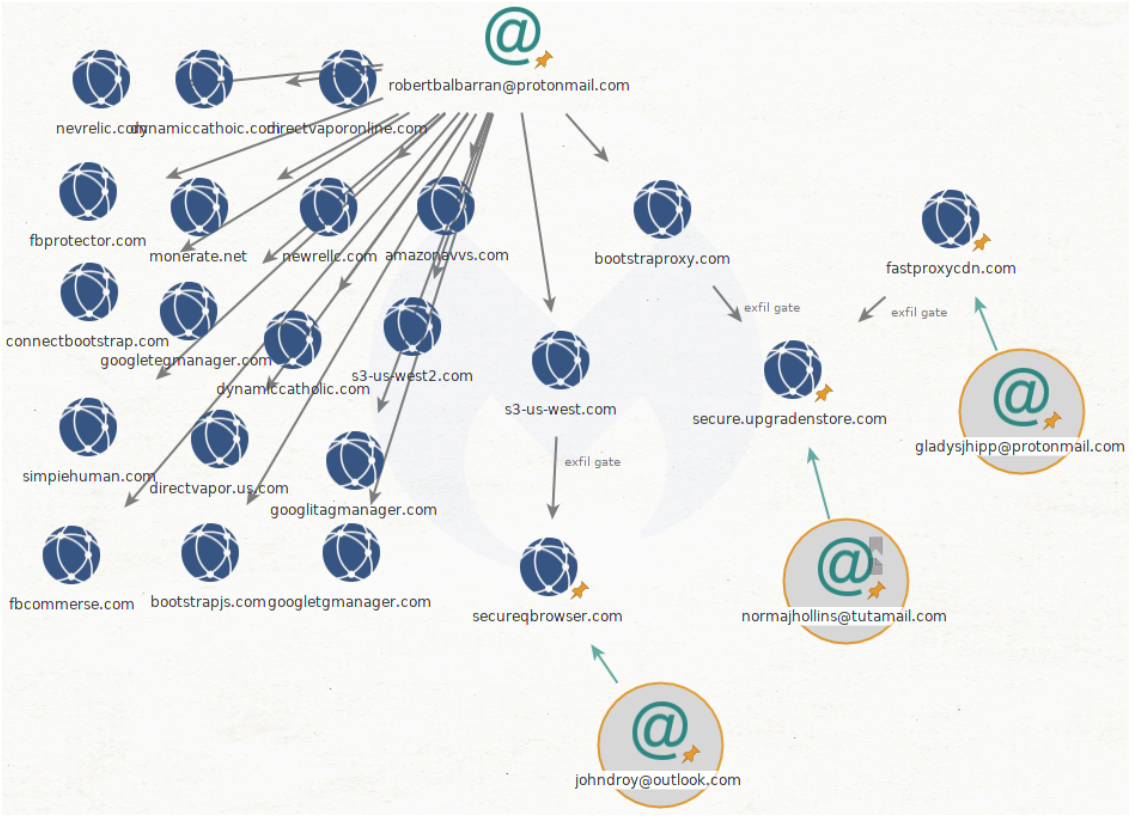


This little code snippet looks for certain keywords associated with a financial transaction and then sends the request and cookie data to the exfiltration server at secureqbrowser[.]com. An almost exact copy of this script was described by Denis Sinegubko of Sucuri in his post Autoloaded Server-Side Swiper.

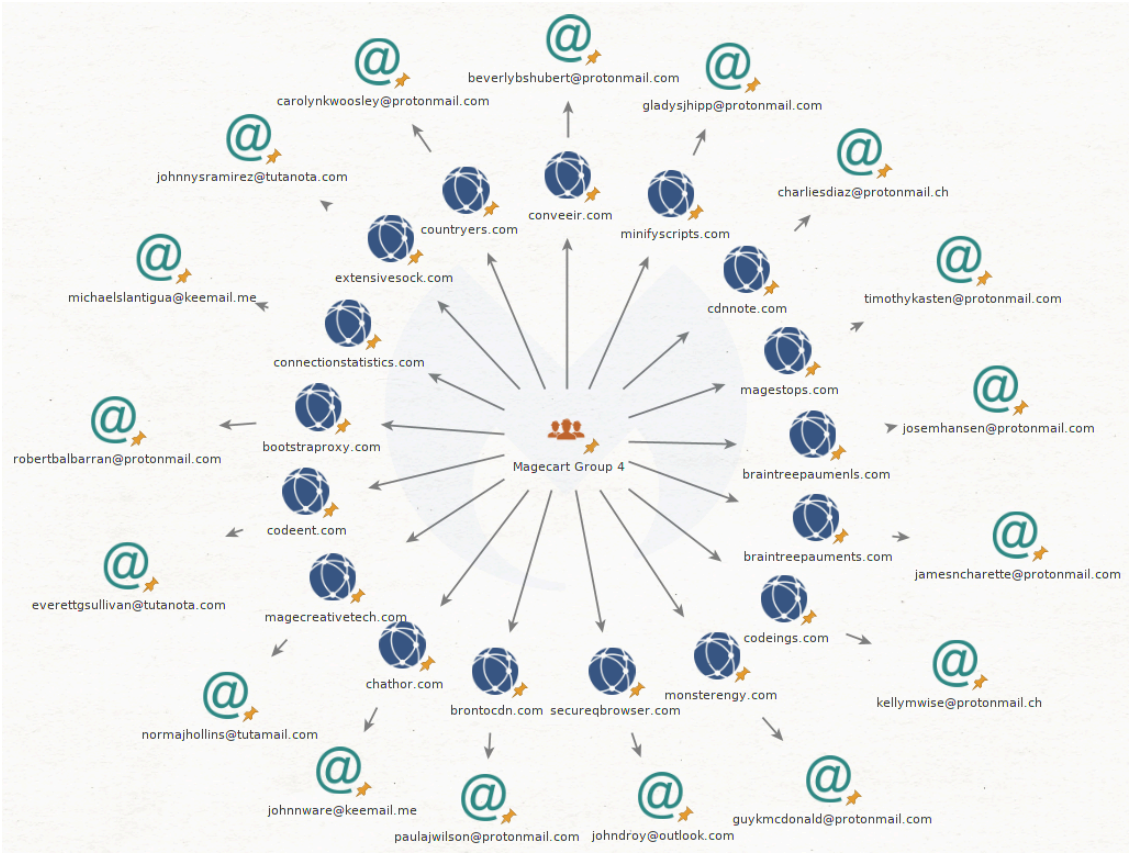
Connections between email registrants and exfiltration gates

Both the client-side and server-side skimmer domains illustrated above (bootstraproxy[.]com and s3-us-west[.]com) are registered to robertbalbarran@protonmail.com. They are listed by RiskIQ under Magecart Group 4: Never gone, simply advancing IOCS.

By checking their exfiltration gates (secure.upgradenstore[.]com and secureqbrowser[.]com), we connected them to other registrant emails and saw a pattern emerge.



Email addresses used to register Magecart domains belonging to Magecart Group 4 contain a [first name], [initial], and [last name]. Expanding our search to other domains used by Group 4 and searching through HYAS' Comox data set, we see this trend continues:



About Cobalt Group

Cobalt Group came to the forefront of public attention in summer 2016 with their “jackpotting” attacks against financial institutions in Europe, which reportedly netted the group over $3 million. Since that time, they have purportedly amassed over a billion dollars from global institutions, evolving their tactics, techniques, and procedures as they go.

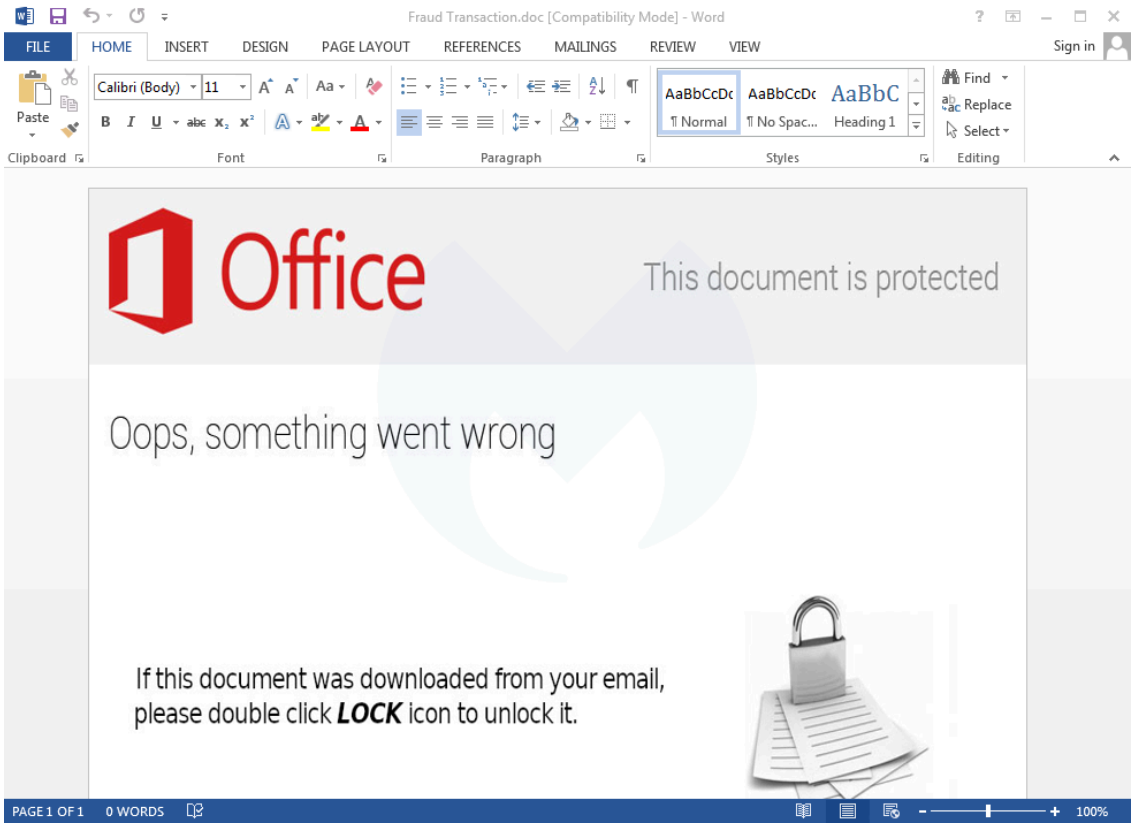
Cobalt Domain Registration and other TTPs

While changing tactics as they have evolved, an identifiable pattern in email naming conventions historically used by Cobalt allowed HYAS to not only identify previous campaign domains, but helped link Cobalt Group campaigns to the Magecart domains identified above.

A small shift from one of their previous conventions of [firstname],[lastname], [fournumbers] (overwhelmingly using protonmail accounts, with a handful of tutanota/keemail.me email accounts) changed to the above-noted convention of [firstname], [initial], [lastname] again using the same email services and registrars, and notably the same use of privacy protection services.

Given the use of privacy services for all the domains in question, it is highly unlikely that this naming convention would be known to any other actor besides those who registered both the Cobalt Group and Magecart infrastructure. In addition, further investigation revealed that regardless of the email provider used, 10 of the seemingly separate accounts reused only two different IP addresses, even over weeks and months between registrations.

One of those emails is petersmelanie@protonmail.com, which was used to register 23 domains, including my1xbet[.]top. This domain was used in a phishing campaign leveraging CVE-2017-0199 with a decoy document called Fraud Transaction.doc.



The same petersmelanie@protonmail.com also registered oracle-business[.]com. Similar campaigns against Oracle and various banks have been attributed to Cobalt Group, with, for example, the domain oracle-system[.]com.

A growing threat requires ongoing work

Based on their historical ties to the space, and the entrance of sophisticated actor groups such as FIN6 and others, it's logical to conclude that Cobalt Group would also enter this field and continue to diversify their criminal efforts against global financial institutions.

The use of both client-side and server-side skimmers and the challenges this poses in identifying Magecart compromises by advanced threat groups necessitates the ongoing work of industry partners to help defend against this significant and growing threat. On that note, the authors of this post would like to recognize the substantial contribution that industry researchers and law enforcement officials are making to combat groups like Cobalt, and hope that the information contained within adds to this corpus of knowledge and further strengthens these efforts.

Indicators of Compromise (IOCs)

Client-side skimmer

urlscan.io archive

Server-side skimmer

urlscan.io archive

Registrant emails associated with Magecart Group 4 domains

robertbalbarran@protonmail.com
josemhansen@protonmail.com
jamesncharette@protonmail.com
paulajwilson@protonmail.com
charliesdiaz@protonmail.ch
johnnware@keemail.me
everettgsullivan@tutanota.com
kellymwise@protonmail.ch
michaelslantigua@keemail.me
beverlybshubert@protonmail.com
carolynkwoosley@protonmail.com
johnnysramirez@tutanota.com
normajhollins@tutamail.com
timothykasten@protonmail.com
gladysjhipp@protonmail.com
guykmcdonald@protonmail.com
johndroy@outlook.com

Registrant emails associated with Cobalt domains

petersmelanie@protonmail.com
jasoncantrell1996@protonmail.com

Cobalt domains registered with Magecart email naming convention

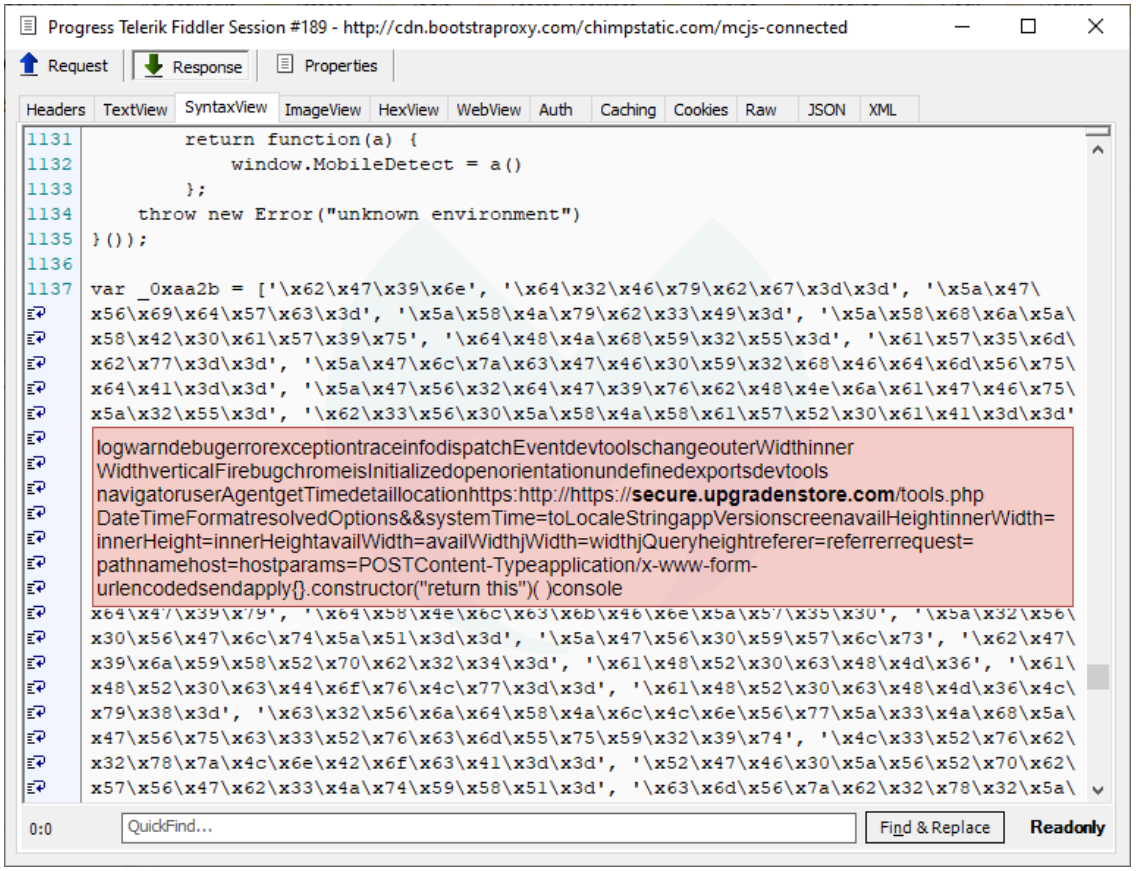
oracle-business[.]com
my-1xbet[.]com
sbeibank[.]online
curacaoegaming[.]site
my1xbet[.]top
newreg[.]site
sbepbank[.]com
orkreestr[.]com
orkreestr[.]host
sbersafe[.]top
aoreestr[.]site
newreg[.]host
sbeibank[.]com
sbelbank[.]com
aoreestr[.]online
curacaoegaming[.]online
sbepbank[.]online

sbelbank[.]online
curacao-egaming[.]online
my1xbet[.]online
orkreestr[.]press
newreg[.]online
aoreestr[.]com

Previous FIN7 domains identified through naming conventions

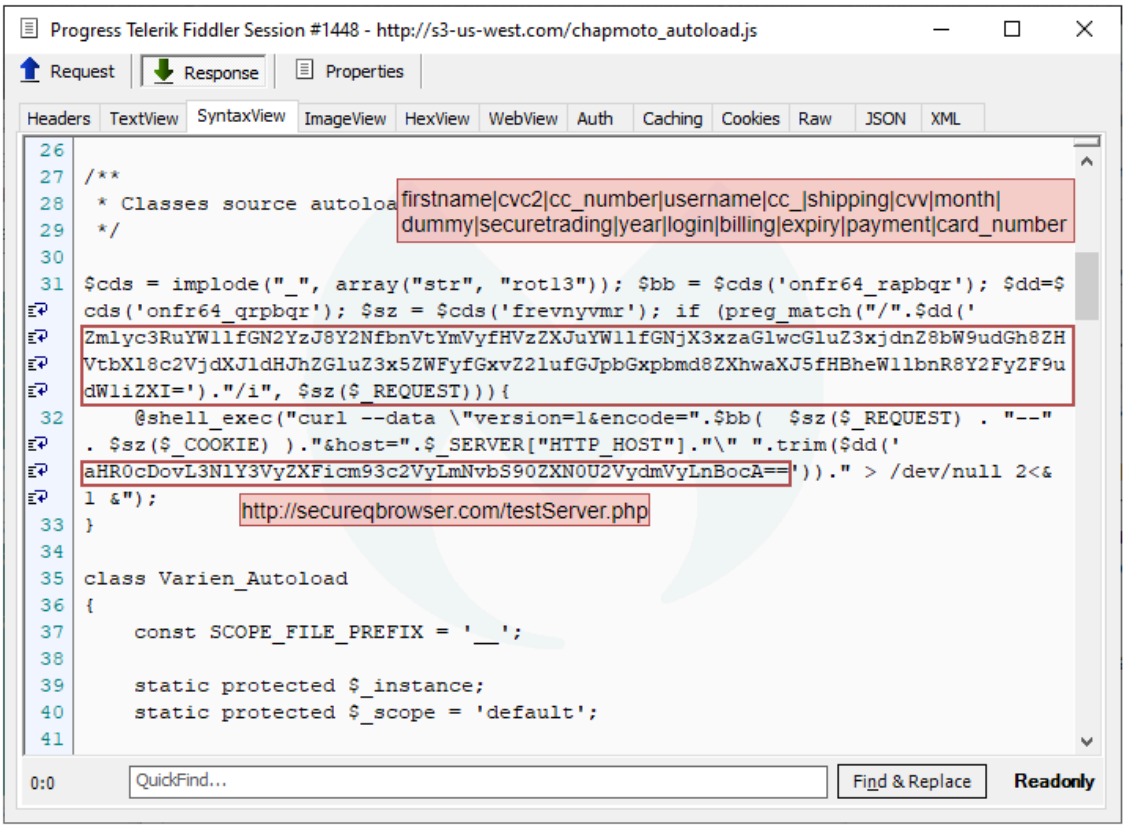
akamaiservice-cdn[.]com
appleservice-cdn[.]com
bing-cdn[.]com
booking-cdn[.]com
cdn-googleapi[.]com
cdn-skype[.]com
cdn-yahooapi[.]com
cdnj-cloudflare[.]com
cisco-cdn[.]com
cloudflare-cdn-r5[.]com
digicert-cdn[.]com
exchange-cdn[.]com
facebook77-cdn[.]com
globaltech-cdn[.]com
gmail-cdn3[.]com
googl-analytic[.]com
google-services-s5[.]com
hpservice-cdn[.]com
infosys-cdn[.]com
instagram-cdn[.]com
live-cdn2[.]com
logitech-cdn[.]com
msdn-cdn[.]com
msdn-update[.]com
mse-cdn[.]com
mse-cdn[.]com
pci-cdn[.]com
realtek-cdn[.]com
servicebing-cdn[.]com
servicebing-cdn[.]com
testing-cdn[.]com
tw32-cdn[.]com
vmware-cdn[.]com

windowsupdatemicrosoft[.]com
yahooservices-cdn[.]com



Server-side skimmer

While checking infrastructure related to Magecart Group 4, we identified a PHP script (see IOCs for the full template) that was perhaps mistakenly served as JavaScript instead. Indeed, access to the backend server would normally be required to view this kind of file.

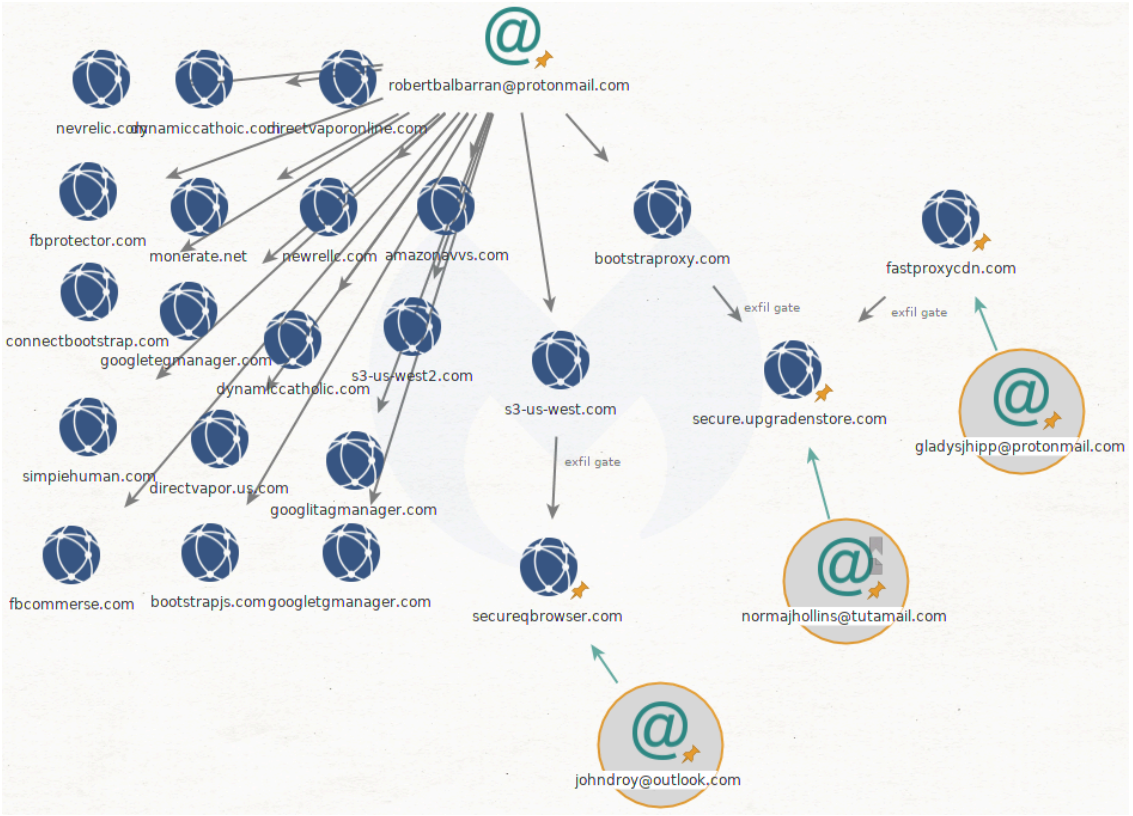


This little code snippet looks for certain keywords associated with a financial transaction and then sends the request and cookie data to the exfiltration server at secureqbrowser[.]com. An almost exact copy of this script was described by Denis Sinegubko of Sucuri in his post Autoloaded Server-Side Swiper.

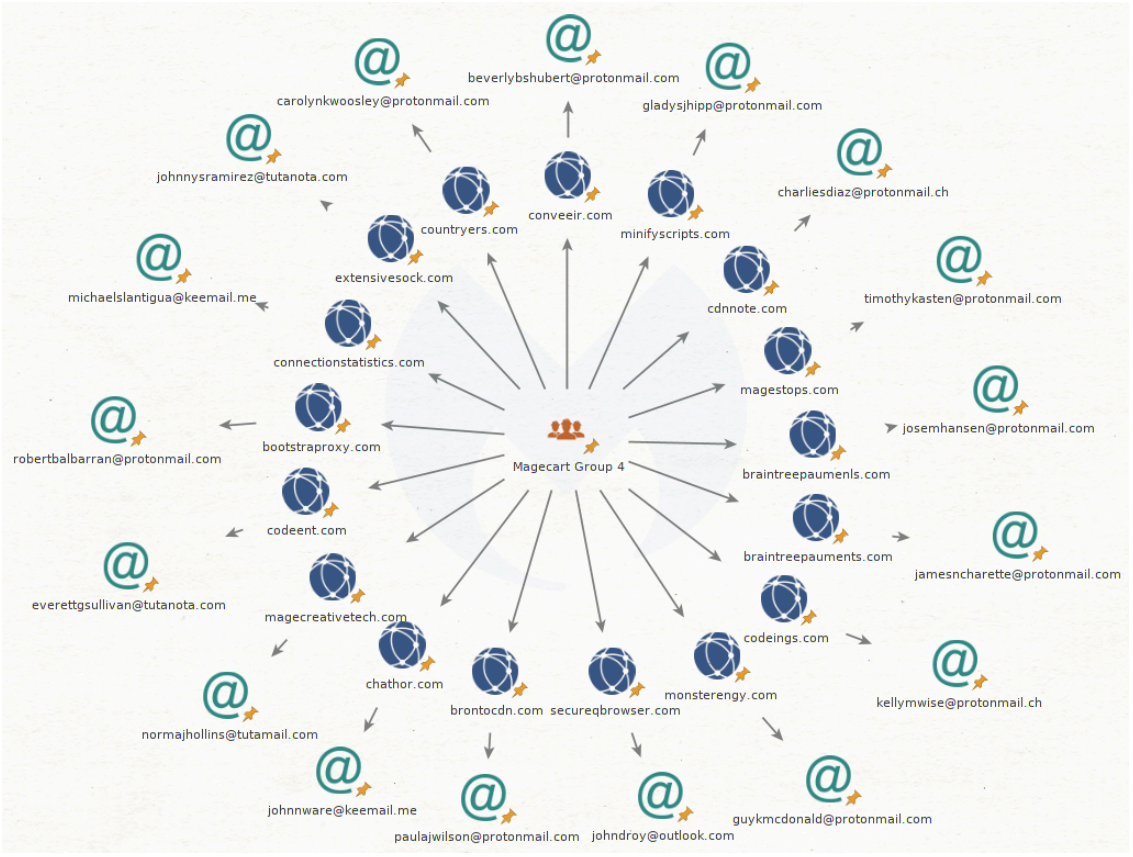
Connections between email registrants and exfiltration gates

Both the client-side and server-side skimmer domains illustrated above (bootstraproxy[.]com and s3-us-west[.]com) are registered to robertbalbarran@protonmail.com. They are listed by RiskIQ under Magecart Group 4: Never gone, simply advancing IOCS.

By checking their exfiltration gates (secure.upgradenstore[.]com and secureqbrowser[.]com), we connected them to other registrant emails and saw a pattern emerge.



Email addresses used to register Magecart domains belonging to Magecart Group 4 contain a [first name], [initial], and [last name]. Expanding our search to other domains used by Group 4 and searching through HYAS' Comox data set, we see this trend continues:



About Cobalt Group

Cobalt Group came to the forefront of public attention in summer 2016 with their “jackpotting” attacks against financial institutions in Europe, which reportedly netted the group over $3 million. Since that time, they have purportedly amassed over a billion dollars from global institutions, evolving their tactics, techniques, and procedures as they go.

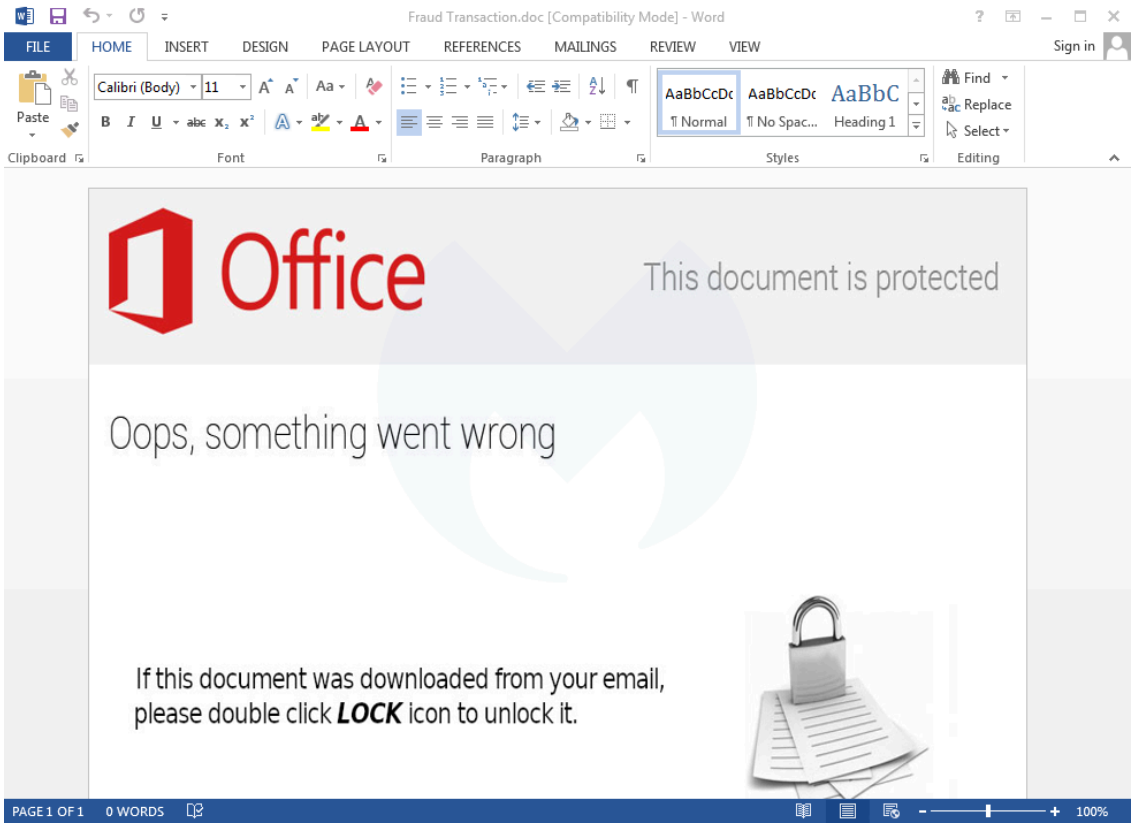
Cobalt Domain Registration and other TTPs

While changing tactics as they have evolved, an identifiable pattern in email naming conventions historically used by Cobalt allowed HYAS to not only identify previous campaign domains, but helped link Cobalt Group campaigns to the Magecart domains identified above.

A small shift from one of their previous conventions of [firstname],[lastname], [fournumbers] (overwhelmingly using protonmail accounts, with a handful of tutanota/keemail.me email accounts) changed to the above-noted convention of [firstname], [initial], [lastname] again using the same email services and registrars, and notably the same use of privacy protection services.

Given the use of privacy services for all the domains in question, it is highly unlikely that this naming convention would be known to any other actor besides those who registered both the Cobalt Group and Magecart infrastructure. In addition, further investigation revealed that regardless of the email provider used, 10 of the seemingly separate accounts reused only two different IP addresses, even over weeks and months between registrations.

One of those emails is petersmelanie@protonmail.com, which was used to register 23 domains, including my1xbet[.]top. This domain was used in a phishing campaign leveraging CVE-2017-0199 with a decoy document called Fraud Transaction.doc.



The same petersmelanie@protonmail.com also registered oracle-business[.]com. Similar campaigns against Oracle and various banks have been attributed to Cobalt Group, with, for example, the domain oracle-system[.]com.

A growing threat requires ongoing work

Based on their historical ties to the space, and the entrance of sophisticated actor groups such as FIN6 and others, it's logical to conclude that Cobalt Group would also enter this field and continue to diversify their criminal efforts against global financial institutions.

The use of both client-side and server-side skimmers and the challenges this poses in identifying Magecart compromises by advanced threat groups necessitates the ongoing work of industry partners to help defend against this significant and growing threat. On that note, the authors of this post would like to recognize the substantial contribution that industry researchers and law enforcement officials are making to combat groups like Cobalt, and hope that the information contained within adds to this corpus of knowledge and further strengthens these efforts.

Indicators of Compromise (IOCs)

Client-side skimmer

urlscan.io archive

Server-side skimmer

urlscan.io archive

Registrant emails associated with Magecart Group 4 domains

robertbalbarran@protonmail.com
josemhansen@protonmail.com
jamesncharette@protonmail.com
paulajwilson@protonmail.com
charliesdiaz@protonmail.ch
johnnware@keemail.me
everettgsullivan@tutanota.com
kellymwise@protonmail.ch
michaelslantigua@keemail.me
beverlybshubert@protonmail.com
carolynkwoosley@protonmail.com
johnnysramirez@tutanota.com
normajhollins@tutamail.com
timothykasten@protonmail.com
gladysjhipp@protonmail.com
guykmcdonald@protonmail.com
johndroy@outlook.com

Registrant emails associated with Cobalt domains

petersmelanie@protonmail.com
jasoncantrell1996@protonmail.com

Cobalt domains registered with Magecart email naming convention

oracle-business[.]com
my-1xbet[.]com
sbeibank[.]online
curacaoegaming[.]site
my1xbet[.]top
newreg[.]site
sbepbank[.]com
orkreestr[.]com
orkreestr[.]host
sbersafe[.]top
aoreestr[.]site
newreg[.]host
sbeibank[.]com
sbelbank[.]com
aoreestr[.]online
curacaoegaming[.]online
sbepbank[.]online

sbelbank[.]online
curacao-egaming[.]online
my1xbet[.]online
orkreestr[.]press
newreg[.]online
aoreestr[.]com

Previous FIN7 domains identified through naming conventions

akamaiservice-cdn[.]com
appleservice-cdn[.]com
bing-cdn[.]com
booking-cdn[.]com
cdn-googleapi[.]com
cdn-skype[.]com
cdn-yahooapi[.]com
cdnj-cloudflare[.]com
cisco-cdn[.]com
cloudflare-cdn-r5[.]com
digicert-cdn[.]com
exchange-cdn[.]com
facebook77-cdn[.]com
globaltech-cdn[.]com
gmail-cdn3[.]com
googl-analytic[.]com
google-services-s5[.]com
hpservice-cdn[.]com
infosys-cdn[.]com
instagram-cdn[.]com
live-cdn2[.]com
logitech-cdn[.]com
msdn-cdn[.]com
msdn-update[.]com
mse-cdn[.]com
mse-cdn[.]com
pci-cdn[.]com
realtek-cdn[.]com
servicebing-cdn[.]com
servicebing-cdn[.]com
testing-cdn[.]com
tw32-cdn[.]com
vmware-cdn[.]com

windowsupdatemicrosoft[.]com
yahooservices-cdn[.]com

Note: This blog post is a collaboration between the Malwarebytes and HYAS Threat Intelligence teams.

Magecart is a term that has become a household name, and it refers to the theft of credit card data via online stores. The most common scenario is for criminals to compromise e-commerce sites by injecting rogue JavaScript code designed to steal any information entered by victims on the checkout page.

Classifying Magecart threat actors is not an easy task due to the diversity of skimmers and their reuse. The effort of attributing Magecart to "groups" started with RiskIQ and Flashpoint's comprehensive Inside Magecart report released in fall 2018, followed by Group-IB several months later.

Much more recently, information about the actual threat actors behind groups has come forward. For example, IBM publicly identified Group 6 as being FIN6. This is interesting on many levels because it reinforces the idea that existing threat groups have been leveraging their past experiences to apply them to theft in the e-commerce field.

One group that caught our interest is Group 4, which is one of the more advanced cybercriminal organizations. While working jointly with security firm HYAS, we found some interesting patterns in the email addresses used to register domains belonging to Magecart matching those of a sophisticated threat group known as Cobalt Group, aka Cobalt Gang or Cobalt Spider.

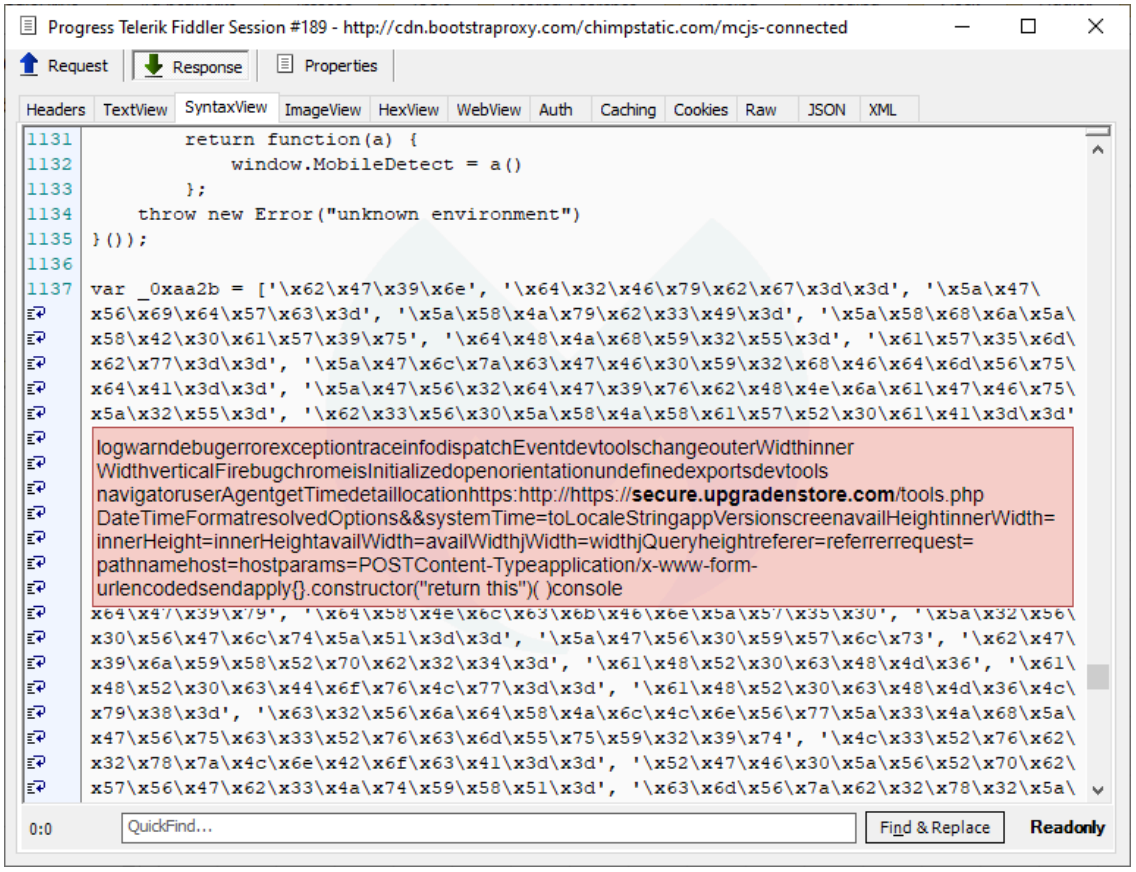
In this blog, we will detail our findings and show that Group 4 was not only conducting client-side skimming via JavaScript but was—and most likely still is—doing the same server-side. This is important to note as most reports about Magecart only cover the former, which is by far easier to identify.

Magecart Group 4

In the *Inside Magecart* report, Group 4 is described as advanced and uses techniques to blend in with normal traffic. For instance, Magecart will register domain names that appear to be tied to advertisers or analytic providers (see IOCs for Cobalt Group domains identified using this TTP and naming convention). Another interesting aspect from the report is that Group 4 is suspected to have had a history in banking malware.

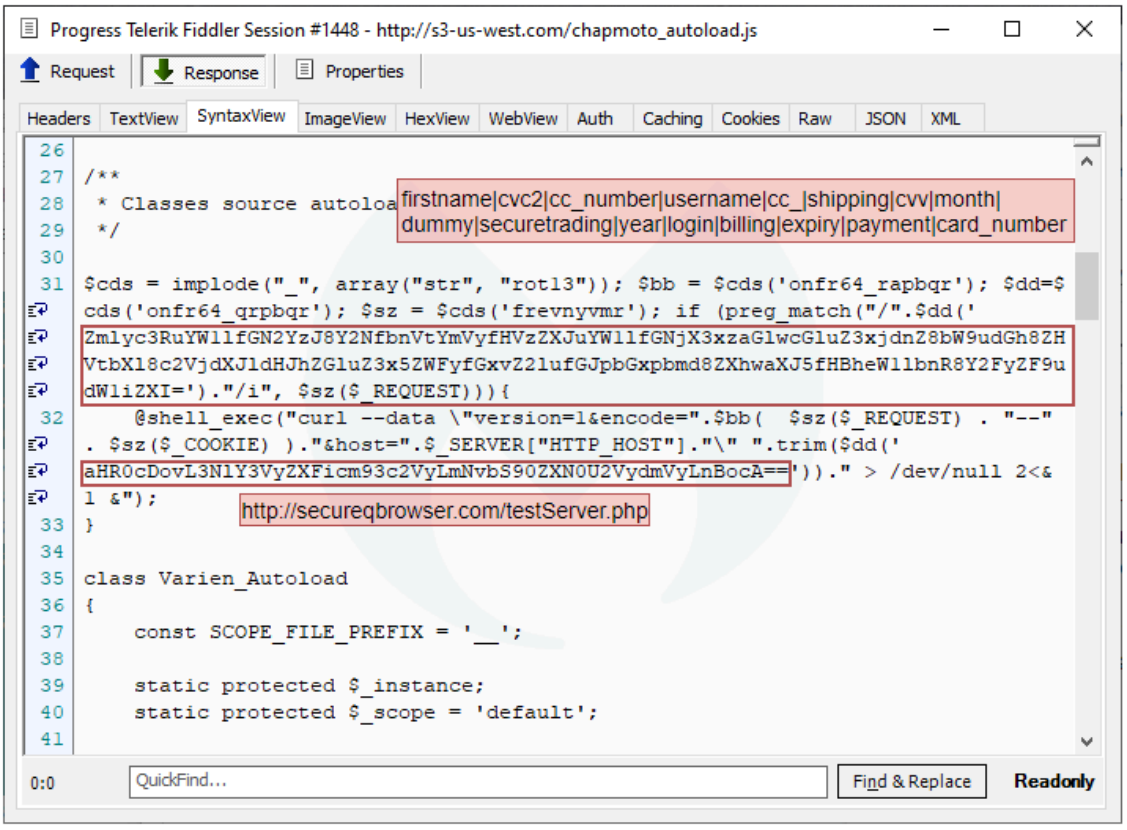
Client-side skimmer

One of Group 4's original skimmers was concealed as the jquery.mask.js plugin (see IOCs for a copy of the script). The malicious code is appended at the end of the script and uses some layers of obfuscation. The hex-encoded data converts to Base64, which can be translated into standard text to reveal skimmer activity and an exfiltration gate.



Server-side skimmer

While checking infrastructure related to Magecart Group 4, we identified a PHP script (see IOCs for the full template) that was perhaps mistakenly served as JavaScript instead. Indeed, access to the backend server would normally be required to view this kind of file.

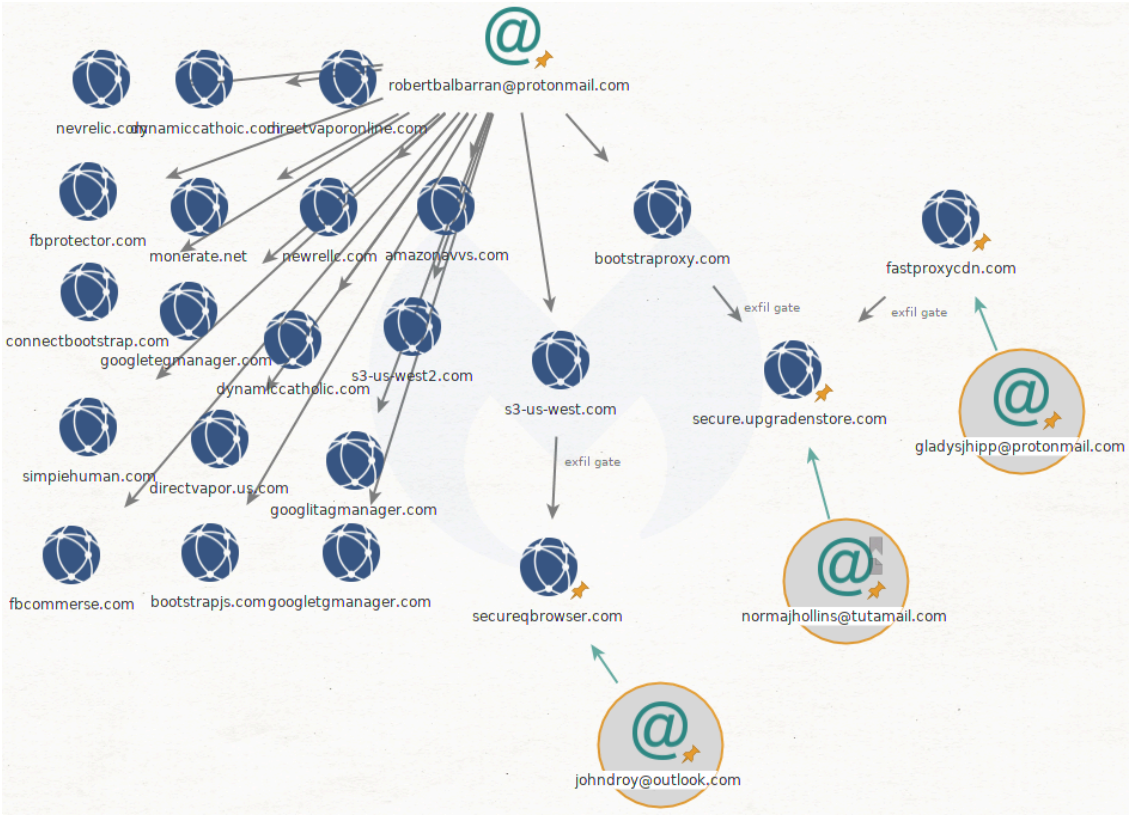


This little code snippet looks for certain keywords associated with a financial transaction and then sends the request and cookie data to the exfiltration server at secureqbrowser[.]com. An almost exact copy of this script was described by Denis Sinegubko of Sucuri in his post Autoloaded Server-Side Swiper.

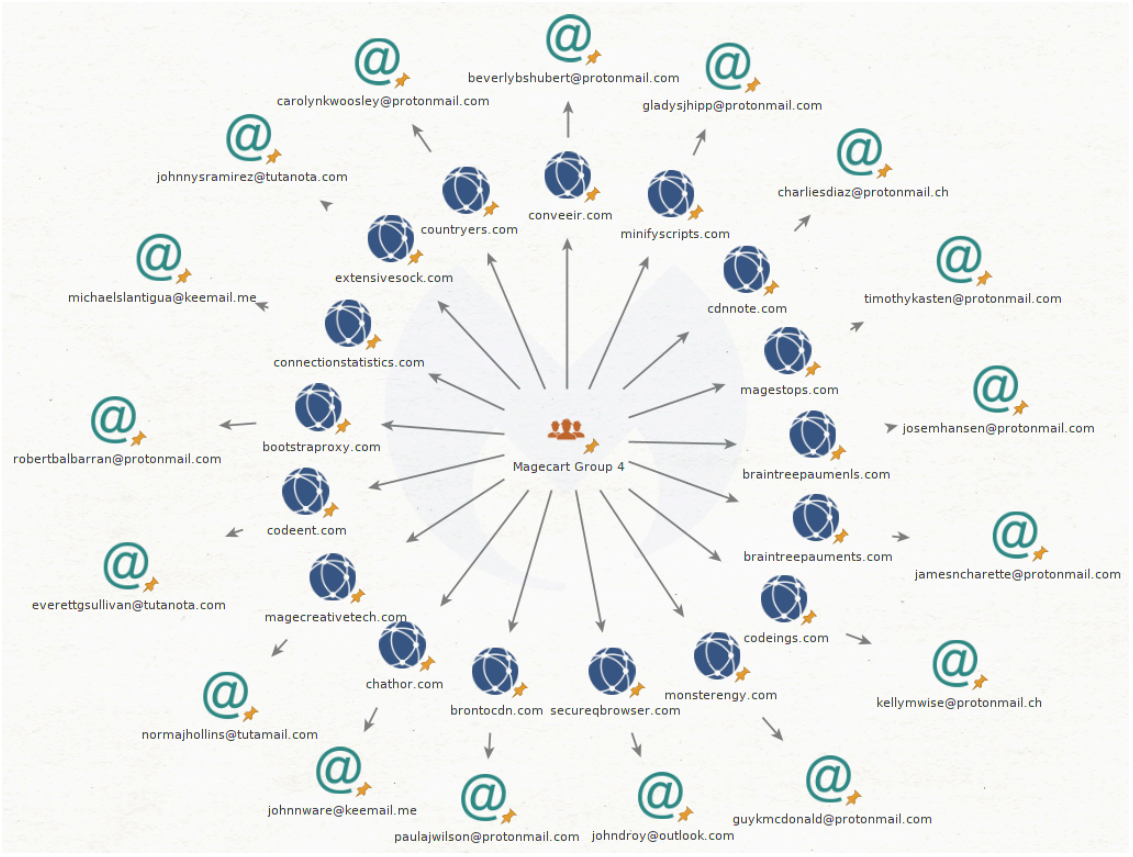
Connections between email registrants and exfiltration gates

Both the client-side and server-side skimmer domains illustrated above (bootstraproxy[.]com and s3-us-west[.]com) are registered to robertbalbarran@protonmail.com. They are listed by RiskIQ under Magecart Group 4: Never gone, simply advancing IOCS.

By checking their exfiltration gates (secure.upgradenstore[.]com and secureqbrowser[.]com), we connected them to other registrant emails and saw a pattern emerge.



Email addresses used to register Magecart domains belonging to Magecart Group 4 contain a [first name], [initial], and [last name]. Expanding our search to other domains used by Group 4 and searching through HYAS' Comox data set, we see this trend continues:



About Cobalt Group

Cobalt Group came to the forefront of public attention in summer 2016 with their “jackpotting” attacks against financial institutions in Europe, which reportedly netted the group over $3 million. Since that time, they have purportedly amassed over a billion dollars from global institutions, evolving their tactics, techniques, and procedures as they go.

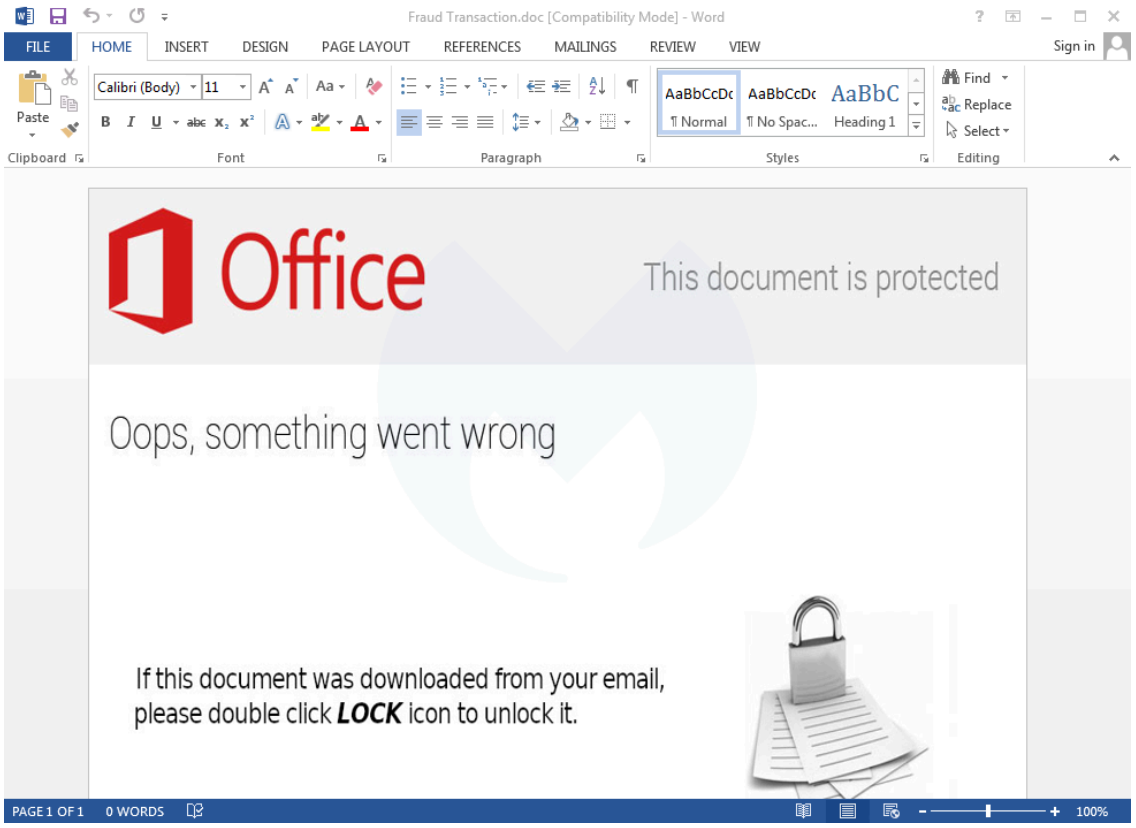
Cobalt Domain Registration and other TTPs

While changing tactics as they have evolved, an identifiable pattern in email naming conventions historically used by Cobalt allowed HYAS to not only identify previous campaign domains, but helped link Cobalt Group campaigns to the Magecart domains identified above.

A small shift from one of their previous conventions of [firstname],[lastname], [fournumbers] (overwhelmingly using protonmail accounts, with a handful of tutanota/keemail.me email accounts) changed to the above-noted convention of [firstname], [initial], [lastname] again using the same email services and registrars, and notably the same use of privacy protection services.

Given the use of privacy services for all the domains in question, it is highly unlikely that this naming convention would be known to any other actor besides those who registered both the Cobalt Group and Magecart infrastructure. In addition, further investigation revealed that regardless of the email provider used, 10 of the seemingly separate accounts reused only two different IP addresses, even over weeks and months between registrations.

One of those emails is petersmelanie@protonmail.com, which was used to register 23 domains, including my1xbet[.]top. This domain was used in a phishing campaign leveraging CVE-2017-0199 with a decoy document called Fraud Transaction.doc.



The same petersmelanie@protonmail.com also registered oracle-business[.]com. Similar campaigns against Oracle and various banks have been attributed to Cobalt Group, with, for example, the domain oracle-system[.]com.

A growing threat requires ongoing work

Based on their historical ties to the space, and the entrance of sophisticated actor groups such as FIN6 and others, it's logical to conclude that Cobalt Group would also enter this field and continue to diversify their criminal efforts against global financial institutions.

The use of both client-side and server-side skimmers and the challenges this poses in identifying Magecart compromises by advanced threat groups necessitates the ongoing work of industry partners to help defend against this significant and growing threat. On that note, the authors of this post would like to recognize the substantial contribution that industry researchers and law enforcement officials are making to combat groups like Cobalt, and hope that the information contained within adds to this corpus of knowledge and further strengthens these efforts.

Indicators of Compromise (IOCs)

Client-side skimmer

urlscan.io archive

Server-side skimmer

urlscan.io archive

Registrant emails associated with Magecart Group 4 domains

robertbalbarran@protonmail.com
josemhansen@protonmail.com
jamesncharette@protonmail.com
paulajwilson@protonmail.com
charliesdiaz@protonmail.ch
johnnware@keemail.me
everettgsullivan@tutanota.com
kellymwise@protonmail.ch
michaelslantigua@keemail.me
beverlybshubert@protonmail.com
carolynkwoosley@protonmail.com
johnnysramirez@tutanota.com
normajhollins@tutamail.com
timothykasten@protonmail.com
gladysjhipp@protonmail.com
guykmcdonald@protonmail.com
johndroy@outlook.com

Registrant emails associated with Cobalt domains

petersmelanie@protonmail.com
jasoncantrell1996@protonmail.com

Cobalt domains registered with Magecart email naming convention

oracle-business[.]com
my-1xbet[.]com
sbeibank[.]online
curacaoegaming[.]site
my1xbet[.]top
newreg[.]site
sbepbank[.]com
orkreestr[.]com
orkreestr[.]host
sbersafe[.]top
aoreestr[.]site
newreg[.]host
sbeibank[.]com
sbelbank[.]com
aoreestr[.]online
curacaoegaming[.]online
sbepbank[.]online

sbelbank[.]online
curacao-egaming[.]online
my1xbet[.]online
orkreestr[.]press
newreg[.]online
aoreestr[.]com

Previous FIN7 domains identified through naming conventions

akamaiservice-cdn[.]com
appleservice-cdn[.]com
bing-cdn[.]com
booking-cdn[.]com
cdn-googleapi[.]com
cdn-skype[.]com
cdn-yahooapi[.]com
cdnj-cloudflare[.]com
cisco-cdn[.]com
cloudflare-cdn-r5[.]com
digicert-cdn[.]com
exchange-cdn[.]com
facebook77-cdn[.]com
globaltech-cdn[.]com
gmail-cdn3[.]com
googl-analytic[.]com
google-services-s5[.]com
hpservice-cdn[.]com
infosys-cdn[.]com
instagram-cdn[.]com
live-cdn2[.]com
logitech-cdn[.]com
msdn-cdn[.]com
msdn-update[.]com
mse-cdn[.]com
mse-cdn[.]com
pci-cdn[.]com
realtek-cdn[.]com
servicebing-cdn[.]com
servicebing-cdn[.]com
testing-cdn[.]com
tw32-cdn[.]com
vmware-cdn[.]com

windowsupdatemicrosoft[.]com
yahooservices-cdn[.]com
